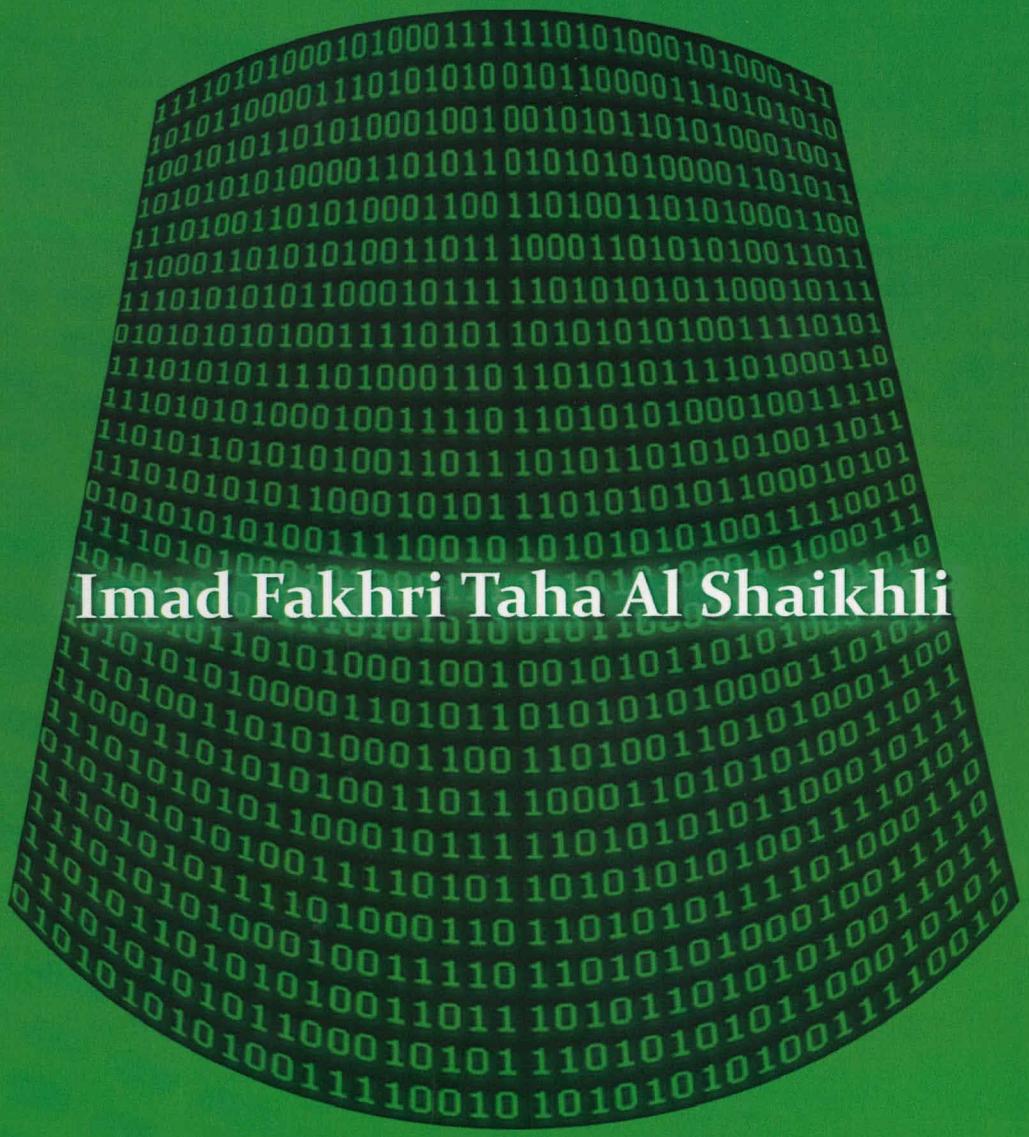
Cryptography

Past, Present and Future

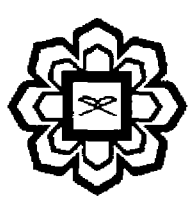


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

TABLE OF CONTENTS

- Sibomana Hilali Hussein

7. Advanced Encryption Standard (AES)

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

ABSTRACT

In this article we will talk about the background of Advanced Encryption Standard (AES), description of AES and how we will encrypt the plaintext and decrypt the cipher text using that cipher. Also we will introduce into algorithm of AES and the cryptanalysis of AES.

DESCRIPTION OF AES

In January 1997, the National Institute of Standards and Technology (NIST) started an open selection process for a new encryption standard. The NIST encouraged parties worldwide to submit proposals for the new standard. The proposals were required to support a block size of at least 128 bits, and three key sizes of 128, 192 and 256 bits.The selection process was divided into two rounds. In the first round, 15 of the submitted 21 proposals were accepted as AES candidates. The candidates were evaluated by a public discussion. The international cryptographic community was asked for comments on the proposed block ciphers. Five candidates were chosen for the second round: MARS (IBM), RC6 (RSA), Rijndael (Daemen and Rijmen), Serpent (Anderson, Biham and Knudsen) and Twofish (Counterpane). Three